| NODIS Library | Legal Policies(2000s) | Search |

NASA Procedural Requirements

NPR 2841.1

Effective Date: January 06, 2011
Expiration Date: January 06, 2016

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change   (NASA Only)

Subject: Identity, Credential, and Access Management

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

Chapter 1. Description of Identity, Credential, and Access Management Services

1.1 Identity management services support identity life-cycle management, identity maintenance, and directory services as described below.

1.1.1 Identity life-cycle management services ensure that people are properly vetted based on their affiliation with NASA and the NASA facilities and systems to which they require access.

1.1.1.1 Identity life-cycle management services provide the ability to create, modify, vet, and retire the identities of people who access NASA facilities and systems.

1.1.1.2 Identity life-cycle management services provide a Level of Confidence (LoC) in a person's identity that can be measured against the Level of Risk (LoR) of access to a physical or logical asset.

1.1.1.3 Identity life-cycle management includes the management of federated identities from trusted identity providers both within and outside the Federal Government.

1.1.2 Identity maintenance services ensure that people can be found in NASA directories to support the conduct of NASA business.

1.1.2.1 Identity maintenance services provide the capability for people to change information about themselves. Examples include nicknames, display names, and NASA location information.

1.1.3 Directory services allow persons and non-person entities (NPEs) to search and retrieve information about people affiliated with NASA.

1.1.3.1 Directories leverage data from identity management and maintenance services discussed in Sections 1.1.1 and 1.1.2.

1.2 Credential management services support credential life-cycle management and certificate management as described below.

1.2.1 Credential life-cycle management services ensure that Agency credentials are issued, re-issued, suspended, or revoked based on affiliation and LoC information provided by authoritative identity management services.

1.2.1.1 Credential life-cycle management services also ensure that Agency credentials are issued using business processes that provide the required Level of Assurance (LoA) defined for the credential by NASA in the ICAM Services Handbook, based on NIST SP 800-63, Electronic Authentication Guidance [800-63].

1.2.1.2 Credentials are issued to allow access to both physical and logical assets throughout NASA.

1.2.2 Certificate management services ensure that Public Key Infrastructure (PKI) certificates for authentication, encryption, and signing operations are issued and maintained in accordance with the x.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework.

1.2.3 Certificate management services ensure that PKI certificates are issued, re-issued, suspended, and revoked based on affiliation and LoC information provided by authoritative identity management services.

1.2.3.1 Certificate management services provide PKI certificates for both persons and NPEs.

1.3 Access management services support asset management, community management, permission management, and authentication and authorization services for both physical and logical (IT) access, as described below.

1.3.1 Asset management services are provided to ensure the proper identification and registration of NASA's assets and the attributes needed for access management.

1.3.2 Community management services support the creation, modification, suspension, and disablement of communities of people who require access to assets or asset groups.

1.3.3 Permission management services ensure that access is granted to assets as required for a person to fulfill his or her assignment.

1.3.3.1 Approval-based permission services allow people to request access to NASA assets for themselves or others.

1.3.3.2 Basic Levels of Entitlement (BLEs) allow access to be granted to people based on communities and other attributes maintained in the Agency's identity management service. Access may be granted based on a person's relationship with NASA (e.g., civil servant, contractor, partner); discipline (e.g., scientist, engineer), or affiliation with a particular NASA organization.

1.3.4 Authentication services ensure that the person or NPE attempting to access an asset matches an asserted identity at the appropriate LoA.

1.3.4.1 Person-based authentication services ensure that persons attempting to access a NASA facility or system is who they claim to be at the appropriate LoA.

1.3.4.2 NPE authentication services validate that the NPE accessing the NASA IT infrastructure is a trusted entity.

1.3.5 Authorization services ensure that the person or NPE attempting to access the asset has a right to do so.

1.3.6 The Certificate Validation Service (CVS) is the authoritative source of valid PKI certificates.

1.3.6.1 The CVS provides status of revocation and expiration of previously issued PKI certificates.

1.3.6.2 The CVS is updated in near real time to increase the confidence that a person or NPE accessing a NASA asset is still eligible for the attempted access.

DISTRIBUTION:
NODIS